UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/771,836	02/03/2004	Lauri Paatero	915-008.020	9737

4955   7590   10/15/2009
WARE FRESSOLA VAN DER SLUYS & ADOLPHSON, LLP
BRADFORD GREEN, BUILDING 5
755 MAIN STREET, P O BOX 224
MONROE, CT 06468

EXAMINER
CHEN, SHIN HON

ART UNIT	PAPER NUMBER
2431	

MAIL DATE	DELIVERY MODE
10/15/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

PTOL-90A (Rev. 04/07)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.
- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on <u>21 May 2009</u>.
2a)☐ This action is **FINAL**.   2b)☒ This action is non-final.
3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) <u>1-32</u> is/are pending in the application.
    4a) Of the above claim(s) _____ is/are withdrawn from consideration.
5)☐ Claim(s) _____ is/are allowed.
6)☒ Claim(s) <u>1-32</u> is/are rejected.
7)☐ Claim(s) _____ is/are objected to.
8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.
10)☒ The drawing(s) filed on <u>03 February 2004</u> is/are: a)☒ accepted or b)☐ objected to by the Examiner.
    Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
    Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
    a)☒ All   b)☐ Some * c)☐ None of:
      1.☒ Certified copies of the priority documents have been received.
      2.☐ Certified copies of the priority documents have been received in Application No. _____.
      3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
    * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08)
    Paper No(s)/Mail Date <u>4/17/09</u>.

4) ☐ Interview Summary (PTO-413)
    Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1.   Claims 1-24 have been examined.

Information Disclosure Statement

2.   The information disclosure statement (IDS) submitted on 4/17/09 is being considered by

the examiner.

Claim Rejections - 35 USC § 103

3.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

4.   Claims 1-3, 8-10 and 22-28 are rejected under 35 U.S.C. 103(a) as being unpatentable

over Cassagnol et al. U.S. Pub. No. 20020129245 (hereinafter Cassagnol) in view of Alve U.S.

Pub. No. 20040101141 (hereinafter Alve).

5.   As per claim 1, Cassagnol discloses a method comprising:

        receiving, in a secure environment in a terminal, first key for decrypting said encrypted

application (Cassagnol: [0012]: use first key to decrypt encrypted data);

        decrypting, in the secure environment, said encrypted application (204) by means of said

first key (Cassagnol: [0025]: decrypt with first whitening key);

re-encrypting, in said secure environment, the application by means of a second key

(Cassagnol: [0025]: re-encrypt data with second whitening key); and

storing, outside said secure environment, the re-encrypted application (Cassagnol:

[0043]: the re-encrypted information is stored externally).

Cassagnol does not clearly disclose the first key is received via a secure channel from a

server outside said terminal. However, Alve discloses securely loading encrypted private key

into the secure processing environment and decrypting it with firs global secret key (Alve:

[0043]). It would have been obvious to one having ordinary skill in the art to securely load

communication key into a secure environment by a cryptographic system provider because both

prior art disclose method of protecting communication data in a distributed network. Therefore,

it would have been obvious o one having ordinary skill in the art at the time of applicant's

invention to combine the teachings of Alve within the system of Cassagnol because it allows

keys to be updated by cryptographic providers.

6.   As per claim 2, Cassagnol as modified discloses a method comprising:

receiving an encrypted application in a terminal (Cassagnol: [0011]: receive encrypted

information);

receiving, in a secure environment in said terminal, via a secure channel, from a server

outside said terminal, a first key for decrypting said encrypted application (Cassagnol: [0111]-

[0112]: receiving key from key server through secure channel);

encrypting, in said secure environment, said first key by means of a second key

(Cassagnol: [0058] and [0061]-[0062]: the encrypted master key/encrypted first key can be

decrypted using device key/second key); and

storing, outside said secure environment, the encrypted first key (Cassagnol: [0058]: the

whitening keys are stored outside of the secure environment).

7.   As per claim 3, Cassagnol as modified discloses the method according to claim 1.

Cassagnol further discloses encrypting, in said secure environment (205), said first key by means

of the second key; and storing, outside said secure environment (205), the encrypted first key

(Cassagnol: [0058]: keys are encrypted and stored externally).

8.   As per claim 8, Cassagnol discloses an apparatus comprising:

an application including an installation part for receiving, a first key for decrypting said

encrypted application (Cassagnol: [0111]-[0112]: receiving key from key server through secure

channel);

a processor for decrypting, in the secure environment, said encrypted application (204) by

means of said first key (Cassagnol: [0025]: decrypt with first whitening key);

said processor for re-encrypting, in said secure environment, the application by means of

a second key (Cassagnol: [0025]: re-encrypt data with second whitening key); and

memory for storing, outside said secure environment, the re-encrypted application

(Cassagnol: [0043]: the re-encrypted information is stored externally).

Cassagnol does not clearly disclose the first key is received via a secure channel from a server outside said terminal. However, Alve discloses securely loading encrypted private key into the secure processing environment and decrypting it with firs global secret key (Alve: [0043]). It would have been obvious to one having ordinary skill in the art to securely load communication key into a secure environment by a cryptographic system provider because both prior art disclose method of protecting communication data in a distributed network. Therefore, it would have been obvious o one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Alve within the system of Cassagnol because it allows keys to be updated by cryptographic providers.

9.   As per claim 9, Cassagnol as modified discloses an apparatus comprising:

an application including an installation part for receiving, in a secure environment in said terminal, via a secure channel, from a server outside said terminal, a first key for decrypting said encrypted application (Cassagnol: [0111]-[0112]: receiving key from key server through secure channel);

a processor for encrypting, in said secure environment, said first key by means of a second key (Cassagnol: [0058]: the encrypted key is stored externally); and

said processor for storing, outside said secure environment, the encrypted first key (Cassagnol: [0058]).

10.   As per claim 10, Cassagnol as modified discloses the apparatus of claim 8. Cassagnol further discloses wherein said processor is:

for encrypting, in said secure environment (205), said first key by means of the second

key; and storing, outside said secure environment (205), the encrypted first key (Cassagnol:

[0058]: keys are encrypted and stored externally).

11.   As per claim 22, Cassagnol discloses a terminal device comprising:

an installation part of an application (Cassagnol: [0111]: receive the cryptographic key);

and

a secure environment, responsive to said first key from said installation part of said

application for decrypting an encrypted application in said terminal device using said first key

received over said secure channel from said server external to said terminal device (Cassagnol:

[0111]-[0112]: receiving key from key server thorough secure channel to decrypt data within

secure environment).

Cassagnol does not clearly disclose the first key is received via a secure channel from a

server outside said terminal. However, Alve discloses securely loading encrypted private key

into the secure processing environment and decrypting it with firs global secret key (Alve:

[0043]). It would have been obvious to one having ordinary skill in the art to securely load

communication key into a secure environment by a cryptographic system provider because both

prior art disclose method of protecting communication data in a distributed network. Therefore,

it would have been obvious o one having ordinary skill in the art at the time of applicant's

invention to combine the teachings of Alve within the system of Cassagnol because it allows

keys to be updated by cryptographic providers.

12.   As per claim 23, Cassagnol as modified discloses the terminal device of claim 22.

Cassagnol further discloses wherein said first key is encrypted by said server using a second key

belonging to said terminal device for providing said first key from said server to said terminal

device (Cassagnol: [0110]-[0112]: data and key communication between the device and server

are encrypted).

13.   As per claim 24, Cassagnol discloses an integrated circuit for installation in a terminal

comprising:

        a signal processor and a secure environment, said secure environment responsive to a first

key for decrypting an encrypted application within said secure environment (Cassagnol: [0111]-

[0112]: receiving key from key server through secure channel), for executing said decrypted

application within said secure environment (Cassagnol: [0025]: decrypt with first whitening key)

and for encrypting said first key with a second key belonging to said terminal device for storage

outside said secure environment (Cassagnol: [0111]: communication between device and key

server is encrypted with session key/second key) so that said first key can be used again with

said secure environment without need for receipt again of said first key from said server

(Cassagnol: [0112]: the server sends key material to the device/first key).

        Cassagnol does not clearly disclose the first key is received via a secure channel from a

server outside said terminal. However, Alve discloses securely loading encrypted private key

into the secure processing environment and decrypting it with firs global secret key (Alve:

[0043]). It would have been obvious to one having ordinary skill in the art to securely load

communication key into a secure environment by a cryptographic system provider because both

prior art disclose method of protecting communication data in a distributed network. Therefore, it would have been obvious o one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Alve within the system of Cassagnol because it allows keys to be updated by cryptographic providers.

14.   As per claim 25, Cassagnol as modified discloses the method of claim 2. Cassagnol further discloses receiving another encrypted application in the terminal (Cassagnol: [0043]: handling the encrypted software within the secure environment); loading the encrypted first key from outside said secure environment (Cassagnol: [0058]: the key is imported externally for decryption); decrypting the encrypted first key with the second key (Cassagnol: [0061]: the master key is decrypted using device key); and decrypting the other encrypted application with the decrypted first key (Cassagnol: [0061]: the software master key is used to decrypt the application).

15.   As per claim 26, Cassagnol as modified discloses the method of claim 25. Cassagnol further discloses re-encrypting the first key by means of a second key (Cassagnol: [0062]: the EMK/first key is encrypted with device key/second key); and storing, outside said secure environment, the encrypted first key (Cassagnol: [0058]: the encrypted whitening key is typically stored outside the secure environment).

16.   As per claim 27, Cassagnol as modified discloses the apparatus of claim 9. Cassagnol further discloses wherein said installation part is for receiving another encrypted application in

the terminal (Cassagnol: [0043]: handling the encrypted software within the secure

environment); loading the encrypted first key from outside said secure environment (Cassagnol:

[0058]: the key is imported externally for decryption); decrypting the encrypted first key with the

second key (Cassagnol: [0061]: the master key is decrypted using device key); and decrypting

the other encrypted application with the decrypted first key (Cassagnol: [0061]: the software

master key is used to decrypt the application).

17.   As per claim 28, Cassagnol as modified discloses the apparatus of claim 27. Cassagnol

further discloses wherein said processor is further configured to: re-encrypting the first key by

means of a second key (Cassagnol: [0062]: the EMK/first key is encrypted with device

key/second key); and storing, outside said secure environment, the encrypted first key

(Cassagnol: [0058]: the encrypted whitening key is typically stored outside the secure

environment).

Claim Rejections - 35 USC § 103

18.   The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

19.   Claims 4-6, 11-13, 15-17 and 19-20 are rejected under 35 U.S.C. 103(a) as being

unpatentable over Cassagnol in view of Alve and further in view of Matyas et al. U.S. Pat. No.

7051211 (hereinafter Matyas).

20.   As per claim 4, Cassagnol as modified discloses the method according to claim 1.

Cassagnol does not explicitly disclose wherein said second key is symmetric and can be derived

from the application (202). However, Matyas discloses generating a new key for re-encrypting

protected software derived from the software (Matyas: column 10 lines 26-46: new key is

generated from S and K and S is provided along with application). It would have been obvious to

one having ordinary skill in the art to generate a new key based on information provided in the

application because the derived information can be used as a seed in generating new key.

Therefore, it would have been obvious to one having ordinary skill in the art at the time of

applicant's invention to combine the teachings of Matyas within the system of Cassagnol

because it prevents malicious from using the first key by generating a new key based on

additional information.

21.   As per claim 5, Cassagnol as modified discloses the method according to claim 4.

Cassagnol as modified further discloses wherein said second key is comprised in the application

(202) itself (Matyas: column 10 lines 26-46).

22.   As per claim 6, Cassagnol as modified discloses the method according to claim 4.

Cassagnol as modified further discloses wherein said second key is generated in the secure

environment (205) using an application seed (Cassagnol: [0025]: generating new key in the

secure environment).

23.   As per claim 11, Cassagnol as modified discloses the apparatus according to claim 8.
Cassagnol does not explicitly disclose wherein said second key is symmetric and can be derived
from the application (202). However, Matyas discloses generating a new key for re-encrypting
protected software derived from the software (Matyas: column 10 lines 26-46: new key is
generated from S and K and S is provided along with application). It would have been obvious to
one having ordinary skill in the art to generate a new key based on information provided in the
application because the derived information can be used as a seed in generating new key.
Therefore, it would have been obvious to one having ordinary skill in the art at the time of
applicant's invention to combine the teachings of Matyas within the system of Cassagnol
because it prevents malicious from using the first key by generating a new key based on
additional information.

24.   As per claim 12, Cassagnol as modified discloses the apparatus according to claim 11.
Cassagnol as modified further discloses wherein said second key is comprised in the application
(202) itself (Matyas: column 10 lines 26-46).

25.   As per claim 13, Cassagnol as modified discloses the apparatus according to claim 11.
Cassagnol as modified further discloses wherein said second key is generated in the secure
environment (205) using an application seed (Cassagnol: [0025]: generating new key in the
secure environment).

26.   As per claim 15, Cassagnol as modified discloses the method according to claim 2.

Cassagnol does not explicitly disclose wherein said second key is symmetric and can be derived

from the application (202). However, Matyas discloses generating a new key for re-encrypting

protected software derived from the software (Matyas: column 10 lines 26-46: new key is

generated from S and K and S is provided along with application). It would have been obvious to

one having ordinary skill in the art to generate a new key based on information provided in the

application because the derived information can be used as a seed in generating new key.

Therefore, it would have been obvious to one having ordinary skill in the art at the time of

applicant's invention to combine the teachings of Matyas within the system of Cassagnol

because it prevents malicious from using the first key by generating a new key based on

additional information.

27.   As per claim 16, Cassagnol as modified discloses the method according to claim 15.

Cassagnol as modified further discloses wherein said second key is comprised in the application

(202) itself (Matyas: column 10 lines 26-46).

28.   As per claim 17, Cassagnol as modified discloses the method according to claim 15.

Cassagnol as modified further discloses wherein said second key is generated in the secure

environment (205) using an application seed (Cassagnol: [0025]: generating new key in the

secure environment).

29.   As per claim 19, Cassagnol as modified discloses the method according to claim 9.
Cassagnol does not explicitly disclose wherein said second key is symmetric and can be derived
from the application (202). However, Matyas discloses generating a new key for re-encrypting
protected software derived from the software (Matyas: column 10 lines 26-46: new key is
generated from S and K and S is provided along with application). It would have been obvious to
one having ordinary skill in the art to generate a new key based on information provided in the
application because the derived information can be used as a seed in generating new key.
Therefore, it would have been obvious to one having ordinary skill in the art at the time of
applicant's invention to combine the teachings of Matyas within the system of Cassagnol
because it prevents malicious from using the first key by generating a new key based on
additional information.

30.   As per claim 20, Cassagnol as modified discloses the method according to claim 19.
Cassagnol as modified further discloses wherein said second key is comprised in the application
(202) itself (Matyas: column 10 lines 26-46).

31.   Claims 7, 14, 18, 21, and 29-32 are rejected under 35 U.S.C. 103(a) as being unpatentable
over Cassagnol in view of Alve and further in view of Takeuchi et al. U.S. Pat. No. 6647495
(hereinafter Takeuchi).

32.   As per claim 7, Cassagnol as modified discloses the method of claim 1. Cassagnol does
not explicitly disclose wherein multiple keys can be transferred successively on the secure

channel into the secure environment, each key being used to decrypt a corresponding encrypted

application in the secure environment. However, Takeuchi discloses transmitting decryption key

when protected software is transmitted to the program execution program (Takeuchi: figure 1). It

would have been obvious to one having ordinary skill in the art to process different software with

different keys sequentially. Therefore, it would have been obvious to one having ordinary skill in

the art at the time of applicant's invention to combine the teachings of Takeuchi within the

system of Cassagnol because it is well known in the art to process multiple software within a

single processor.

33.   As per claim 14, Cassagnol as modified discloses the apparatus of claim 8. Cassagnol

does not explicitly disclose wherein multiple keys can be transferred successively on the secure

channel into the secure environment, each key being used to decrypt a corresponding encrypted

application in the secure environment. However, Takeuchi discloses transmitting decryption key

when protected software is transmitted to the program execution program (Takeuchi: figure 1). It

would have been obvious to one having ordinary skill in the art to process different software with

different keys sequentially. Therefore, it would have been obvious to one having ordinary skill in

the art at the time of applicant's invention to combine the teachings of Takeuchi within the

system of Cassagnol because it is well known in the art to process multiple software within a

single processor.

34.   As per claim 18, Cassagnol as modified discloses the method of claim 2. Cassagnol does

not explicitly disclose wherein multiple keys can be transferred successively on the secure

channel into the secure environment, each key being used to decrypt a corresponding encrypted

application in the secure environment. However, Takeuchi discloses transmitting decryption key

when protected software is transmitted to the program execution program (Takeuchi: figure 1). It

would have been obvious to one having ordinary skill in the art to process different software with

different keys sequentially. Therefore, it would have been obvious to one having ordinary skill in

the art at the time of applicant's invention to combine the teachings of Takeuchi within the

system of Cassagnol because it is well known in the art to process multiple software within a

single processor.

35.   As per claim 21, Cassagnol as modified discloses the method of claim 9. Cassagnol does

not explicitly disclose wherein multiple keys can be transferred successively on the secure

channel into the secure environment, each key being used to decrypt a corresponding encrypted

application in the secure environment. However, Takeuchi discloses transmitting decryption key

when protected software is transmitted to the program execution program (Takeuchi: figure 1). It

would have been obvious to one having ordinary skill in the art to process different software with

different keys sequentially. Therefore, it would have been obvious to one having ordinary skill in

the art at the time of applicant's invention to combine the teachings of Takeuchi within the

system of Cassagnol because it is well known in the art to process multiple software within a

single processor.

36.   As per claim 29, Cassagnol as modified discloses the method of claim 7. Cassagnol as

modified further disclose wherein said processor is further configured to:

encrypting, in said secure environment, each of said multiple keys by means of the

second key (Cassagnol: [0058] and [0061]-[0062]: the encrypted master key/encrypted first key

can be decrypted using device key/second key); and

storing, outside said secure environment, each of the multiple keys encrypted by the

second key (Cassagnol: [0058]: the whitening keys are stored outside of the secure environment).

37.   As per claim 30, Cassagnol as modified discloses the method of claim 29. Cassagnol as

modified further discloses wherein said installation part is for receiving another encrypted

application in the terminal (Cassagnol: [0043]: handling the encrypted software within the secure

environment); loading the encrypted first key from outside said secure environment (Cassagnol:

[0058]: the key is imported externally for decryption); decrypting the encrypted first key with the

second key (Cassagnol: [0061]: the master key is decrypted using device key); and decrypting

the other encrypted application with the decrypted first key (Cassagnol: [0061]: the software

master key is used to decrypt the application).

38.   As per claim 31, Cassagnol as modified discloses the apparatus of claim 14. Cassagnol as

modified further disclose wherein said processor is further configured to:

encrypting, in said secure environment, each of said multiple keys by means of the

second key (Cassagnol: [0058] and [0061]-[0062]: the encrypted master key/encrypted first key

can be decrypted using device key/second key); and

storing, outside said secure environment, each of the multiple keys encrypted by the

second key (Cassagnol: [0058]: the whitening keys are stored outside of the secure environment).

39.   As per claim 32, Cassagnol as modified discloses the method of claim 29. Cassagnol as

modified further discloses wherein said installation part is for receiving another encrypted

application in the terminal (Cassagnol: [0043]: handling the encrypted software within the secure

environment); loading the encrypted first key from outside said secure environment (Cassagnol:

[0058]: the key is imported externally for decryption); decrypting the encrypted first key with the

second key (Cassagnol: [0061]: the master key is decrypted using device key); and decrypting

the other encrypted application with the decrypted first key (Cassagnol: [0061]: the software

master key is used to decrypt the application).

Response to Arguments

40.   Applicant's arguments with respect to claims 1-32 have been considered but are moot in

view of the new ground(s) of rejection.

Conclusion

41.   The prior art made of record and not relied upon is considered pertinent to applicant's

disclosure.

        Davis U.S. Pat. No. 5805706 discloses method for re-encrypting data without unsecured

exposure of its non-encrypted format.

        Klemba et al. U.S. Pat. No. 7055040 discloses method for uniquely and securely loading

software to an individual computer.

Rusnak et al. U.S. Pat. No. 6098056 discloses method for controlling access rights to and security of digital content in a distributed information system.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to SHIN-HON CHEN whose telephone number is (571)272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, William R. Korzuch can be reached on (571) 272-7589. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

Shin-Hon Chen
Primary Examiner
Art Unit 2431

/Shin-Hon Chen/
Primary Examiner, Art Unit 2431